Question/Answers from the "Understanding the DCSA Security Review and Rating Process (webinar)", Sept. 16, 2021

PRIORITIZATION

Q: When will DCSA begin conducting security reviews using this methodology?

A: Effective September 1, 2021, DCSA began conducting security reviews based upon the refined and communicated security review approach that incorporates best practices from previous security review models. DCSA personnel are scheduling and visiting on-site contractor personnel to review 32 CFR Part 117 NISPOM compliance. DCSA will conduct recurring security reviews to verify the contractor's security program is protecting classified information and implementing the provisions of the NISPOM Rule. The complimentary security rating process is a compliance first model that eliminates enhancements, utilizes a whole company approach based on analysis of the corporate culture, management support from the top, employee awareness, and cooperation within the security community. For more information on the rating process, visit https://www.dcsa.mil/mc/ctp/srrp/.

Q: Section 117.7 of 32 CFR does not define the periodicity of reviews. Is there written guidance stipulating how often security reviews may occur and what requirements must an industrial security representative (ISR) conform to in order to conduct unannounced reviews? When will my facility be reviewed?

A: DCSA will generally provide notice to the contractor of a forthcoming review, but may also conduct unannounced reviews at its discretion. The requirements are internally published and quality controlled. DCSA determines the scope and frequency of security reviews consistent with risk management principles. We strongly encourage you to stay in close contact with your local field office and assigned ISR and proactively report security challenges.

Q: My facility is assigned to NAESOC. How often will we get a security review?

A: The NAESOC is the National Access Elsewhere Security Oversight Center. All National Industrial Security Program (NISP) facilities, including those assigned to NAESOC, are subject to a security review on a regular and recurring basis as operational resources and mission objectives allow. See previous question.

METHODOLOGY

Q: What aspects of the security rating process are the most important?

A: The security rating process is built on two guiding principles: Compliance first and whole-company approach. Compliance first means that there are no enhancements to offset weaknesses. The whole-company approach means that security is not a performance metric of a single position or role. It takes a team of management, security staff, and all contractor personnel to implement a high functioning security program. It is important to remember that Satisfactory

equals compliance. It is the most common security rating and indicates that a facility is in general compliance with the basic terms of the NISPOM. Obtaining a higher than satisfactory rating is not required but shows a commitment to implementing effective security practices to protect classified information, sensitive government information, and technology at your facility.

Q: Is RISO still in place?

RISO, or Risk-based Industrial Security Oversight (RISO), was the formal name given to one of our previous security review methods. Over the last year, DCSA reviewed our security review approach to ensure our oversight methods aligned with updated national and DoD policy. Some of the RISO practices not included in the new security review model:

- Large-scale asset identification (does consider what the contractor is protecting and how it is being protected)
- Cradle to grave walkthrough of critical assets (does consider internal processes throughout classified contract deliverable lifecycles)
- Separate formalized supply chain risk management process (does consider supply chain during internal process review)
- Vulnerabilities not tied to NISPOM compliance (does consider issues/concerns not related to NISPOM compliance as 'observations')
- Security Baseline, POA&M, and Tailored Security Plan (does result in Security Rating Sheet, results letter to management, and FSO Comments)

Q: Will DCSA no longer consider enhancements during the security rating process?

A: The security rating process is a compliance first model that eliminates enhancements and uses a whole company approach to analyze the corporate culture, management support from the top, employee awareness, and cooperation within the security community. Although no longer considered enhancements, many of the best practices conducted by industry will align to the security posture category criteria. Refer to the Security Rating Category Reference Cards to identify ways you can achieve our new standards.

Q: What is the main difference between a critical vulnerability and a serious vulnerability?

A: Both critical and serious vulnerabilities involve risk to classified information. With critical vulnerabilities either classified information has already been lost or compromised, or classified information is at imminent risk of loss or compromise (meaning it is likely to occur at any moment). With serious vulnerabilities, classified information is in danger of loss or compromise (meaning there is a possibility that classified information will be lost or compromised).

Q: Is a serious vulnerability the same as a serious security issue?

A: No. A serious vulnerability is a vulnerability that indicates classified information is in danger of loss or compromise. A serious security issue is a facility security clearance (FCL) relevant vulnerability, whether critical or serious, that without mitigation would affect a facility's ability to obtain and maintain a FCL. These issues may result in an invalidation or revocation. Another

way of explaining the two, all serious security issues are vulnerabilities but not all vulnerabilities are serious security issues.

Q: How does this model apply to non-possessing facilities? Will the process be the same for a virtual review conducted by NAESOC?

A: NAESOC, or the National Access Elsewhere Security Oversight Center, uses the same security review and rating process as the rest of DCSA.

Q: What is the definition of approach vector?

A: An approach vector is a method used to connect an adversary to facility personnel, information, networks, or technology in order to execute an operation. Our industry partners will recognized approach vectors as the Methods of Contact outlined on the Methods of Contact Methods of Operation (MCMO) matrix. Examples include cyber operations, email requests, foreign visits, personal conduct, phishing operations, resumes, social networking; amongst others.

Q: What qualifies a facility as 'complex'?

A: Facilities not assigned to the NAESOC or not eligible for a NAESOC assignment are considered to have complex operations. Key factors considered in this determination include: safeguarding, classified information systems, critical technology (classified or unclassified support), home office facility of a large complex multiple facility organization, and foreign ownership, control or influence (FOCI) mitigation. Facilities with complex operations can have a single isolated vulnerability and still be considered for a superior rating. Facilities without complex operations can have a single isolated vulnerability and still be considered for a commendable rating.

Q: What is the role of interviews in the security review and rating methodology?

A: Interviews with contractor personnel are key to the refined security review and rating models. In fact, the primary means for reviewing internal processes, NISPOM elements, and areas of special emphasis are through interviews with contractor personnel. Not only is DCSA looking at implemented procedures but interviews assist in our review of how effective those procedures are throughout the entire organization.

Q: When will the exit briefing take place to provide the rating? Is the rating assessment completed onsite during the review and the results communicated prior to DCSA's departure or are the results communicated at a later time?

A: DCSA will provide the security rating during the formal exit briefing. In most cases, the exit briefing will not occur on the last day of the on-site review due to necessary coordination. Once the security rating is coordinated, the ISR will work with the facility security officer (FSO) to schedule the formal exit briefing with key contractor personnel (e.g., FSO, senior management official (SMO), insider threat program senior official (ITPSO)).

Q: How do you protect against subjectivity?

A: Our security professionals combine their experience, training, and professional standards with information and knowledge obtained during the security review (also known as evidence) to carefully analyze and assess the results and criteria. This includes making a rating determination using ethical principles of objectivity – not allowing bias, conflict of interest, or the influence of other people to affect their decisions or actions. While we strive for consistency in processes, we also understand outcomes may vary based on facility circumstances. For example, a non-compliance at one facility may place classified information at risk resulting in a vulnerability while the same non-compliance at another facility may not resulting in an administrative finding.

Our security professionals document their rationale for making a determination within their security review report. Then, using our recently updated quality management program, we will continuously monitor consistency throughout the agency, readjust, and train as needed. Make no mistake, ensuring clear professional standards are outlined and achieved is extremely important to DCSA.

Q: Will Controlled Unclassified Information (CUI) be part of the security review?

A: At this time, DCSA will not assess contractor compliance with contractually-established CUI system requirements in DoD classified contracts associated with the NISP.

Q: Will DCSA still use the same process for Cogswell Awards?

A: Yes, there have been no changes to the current Cogswell process.

Q: Will DCSA consider changes to the new rating system if the number of Superior facilities drops significantly?

A: The refined security rating process is aligned to DoDM 5220.22, Volume 2, which has minimum requirements outlined for each security rating level. Under the previous model, enhancements could off-set a vulnerability that placed classified information at risk. This is no longer the case under the refined compliance-first model. DCSA is always looking for ways to improve our processes, however any changes must conform with policy.

RATINGS

Q: Why does DCSA use the lowest category rating to determine the overall security rating instead of taking an average?

A: DODM 5220.22, Volume 2, requires that facilities meet certain requirements to qualify for each level of security rating. For example, a superior rated facility must have consistent, full, and effective NISPOM implementation; sustained high level of management support; documented and implemented procedures which heighten employee awareness; and a spirit of cooperation within the security program. The superior criteria within the four categories define each of those

requirements. Since the facility must meet all the policy requirements to get a superior they must also meet all the associated criteria that defines the requirement to be assigned a superior. As a reminder, the category ratings are only provided for process improvement efforts and to identify successful areas within the security program. The final rating is based on the facility meeting the applicable level criteria in all four categories.

Q: Will a facility still be eligible for a satisfactory rating if a critical vulnerability is discovered during the security review?

A: In order to receive a satisfactory rating, a facility must be in general conformity. General conformity means a facility has no critical vulnerabilities, systemic vulnerabilities, or serious security issues identified during the security review. A critical vulnerability indicates classified information has already been lost or compromised or is at imminent risk of loss or compromise. Due to the seriousness of a critical vulnerability, if identified during the security review DCSA will determine the facility is not in general conformity.

Q: If a facility receives a satisfactory rating, can they expect suggestions from their DCSA ISR to help them improve to a higher rating?

A: Contractors can use category ratings to identify opportunities for improvement or areas of success throughout the security program. ISRs may discuss these ratings during the security review exit briefing. A summary is also provided on the security rating sheet.

Q: If a facility receives a Marginal or Unsatisfactory rating, how long does it take before it affects the contractor's FCL?

A: If the facility has lost the ability to adequately safeguard the classified information in their possession or to which they have access, DCSA will consider the facility for an invalidation or intent to revoke, as necessary. Justified invalidations or the intent to revoke a FCL can occur at any time, not just as a result of a security review.

Q: How many administrative findings can a facility have and still receive a Satisfactory rating?

A: It depends. There are times when administrative findings are elevated to a serious vulnerability, such as when conditions and circumstances indicate intentional disregard of security regulations or a pattern of negligence. For example, a repeat issue that DCSA has notified a facility about on several occasions and no action was taken to mitigate the area of non-compliance or a large number of administrative findings indicating a lack of overall security program.

If an administrative finding is elevated to a serious vulnerability, it would be further characterized as isolated or systemic. If the elevation was due to a repeat issue it would likely result in an isolated serious vulnerability. If the elevation was due to a large number of administrative findings it would likely result in a systemic serious vulnerability. In this case, the facility would not be in general conformity.

Q: Under the old rating system, Marginal and Unsatisfactory ratings impacted a CDCs ability to be awarded and perform on classified contracts. Is this still the same under the new model?

An invalidation or intent to revoke are what impacts a contractor's ability to be awarded and perform on classified contracts (not the marginal or unsatisfactory rating).

Q: Does a non-possessing facility assigned to NAESOC have a possibility of receiving a commendable or superior rating since they don't possess classified on-site?

A: Yes, absolutely. This model was created to provide all facilities, regardless of size or complexity, with an opportunity to achieve a commendable or superior rating. If a facility has complex operations, it can have a single isolated serious vulnerability and be considered for a superior. If a facility does not have complex operations, it can have a single isolated serious vulnerability and be considered for a commendable.

Q: Do facilities have the option to "challenge" the assigned rating? What if the ISR misses something key during their security review?

A: The DCSA security rating is a whole-company approach that focuses on both processes and effective outcomes. In other words, implementing a security process does not indicate the process was effective or consistently applied. When assessing the security rating, DCSA personnel consider the information obtained and knowledge gained during the security review to make an evidentiary-based determination. The rating is not always going to be what the facility expected as the success and weakness are shared throughout the facility from the contractor personnel, to security staff, and management. DCSA fully supports the ISRs to make an objective rating determination. In the rare instance that a facility has justification to challenge a security rating, the FSO or SMO must coordinate their challenge through the responsible Field Office Chief.

Q: In the post-security review artifacts, will only the overall security rating be provided or will the category ratings be given too?

A: The Security Rating Sheet identifies both category ratings and the overall security rating.

Q: Since the rating includes criteria related to classified threat reporting and approach vectors, will facilities receive this information from DCSA? Should facilities use Targeting Technologies briefings to communicate the threat?

A: The facility can receive information related to classified threat reporting from DCSA, other government agencies, or government contracting activities. The Targeting Technologies and associated Methods of Contact Methods of Operation (MCMO) Matrix are great resources to identify approach vectors, determine which methods impact the facility, and implement security controls or measures to counter a potential threat.

Q: Can a parent facility (or home office) receive a Satisfactory but the division site receive a higher level rating?

A: Yes, the security rating is based on security posture at the cleared facility being reviewed.

CRITERIA

Q: How does the ISR compile information to assess each security posture category? Will employees be interviewed?

A: The method of compilation is flexible. DCSA personnel consider information obtained and knowledge gained through employee interviews when assessing each security posture category.

Q: How does the ISR assess the concept of management support? Isn't management support a requirement in the NISPOM Rule?

A: The Senior Management Official (SMO) has responsibilities outlined in the NISPOM which are incorporated into the Satisfactory level rating. The Management Support criteria for Commendable and Superior ratings are written for management and not just the SMO. When assessing the concept of management support, DCSA will use the information and knowledge obtained during the security review to determine if the outlined criteria has (or has not) been met. All criteria must be met at the level to be assigned the rating.

Q: How does the ISR assess the concept of Security Community?

A: When assessing the concept of security community, the ISR will use the information and knowledge obtained during the security review as well as through collaboration with the CI Special Agent and Information Systems Security Professional (ISSP) to determine if the outlined criteria has (or has not) been met.

Q: Can you further define "culture of security"?

A: To 'embed a culture of security' indicates that security is an essential part of the facility's core values. Whereas, to 'implement a culture of security' indicates a standard of security has been put in place.

Q: How does the ISR determine if the SMO has retained accountability?

A: DCSA will assess information obtained (e.g., self-inspection certification) and knowledge gained (e.g., interviews) during security engagements to determine if the SMO has retained accountability of the security program.

Q: I am one of three employees on-site. All others are geographically distributed around the world. How with the ISR interview my employees?

A: Interviews are key to assessing the overall security posture at a facility. DCSA personnel will coordinate with the FSO to ensure the availability of contractor personnel for interviews. The ISR will interview off-site employees through electronic communications (e.g., phone), as needed. If employees are unavailable, DCSA may postpone the exit briefing until the security posture can be adequately assessed.